Claims

1. A memory device being connected to an electronic device fixedly or detachably, comprising:

first memory of non-tamper-resistance having a usual area that can be accessed from the electronic device and a secure area that cannot directly be accessed from the electronic device;

second memory of tamper resistance that cannot directly be accessed from the electronic device; and

a secure control section for managing access to the second memory,

wherein access to the secure area of the first memory from the electronic device can be made only through the secure control section.

2. The memory device according to claim 1, wherein upon reception of a command of the electronic device authenticated by the secure control section, the secure control section accesses the secure area or the second memory and writes or reads data.

3. The memory device according to claim 1 or 2,

wherein a encryption key is stored in the second memory, and

wherein the secure control section encrypts the data to

be written into the secure area using the encryption key and writes the encrypted data and decrypts the data read from the secure area using the encryption key.

4. The memory device according to any one of claims 1 to 3, wherein the secure control section calculates a hash value of the data to be written into the secure area, stores the hash value in the second memory, calculates a hash value of the data read from the secure area, and compares the hash value with the hash value stored in the second memory.

5. The memory device according to claim 1, wherein the usual area of the first memory includes an authentication area that can be accessed only by electronic devices authenticated by a general control section for controlling the memory device and a non-authentication area that can be accessed even by an electronic device not authenticated.

6. The memory device according to any one of claims 1 to 5, wherein boundary address information indicating the boundary between the usual area and the secure area and logical-physical address translation tables describing the relationship between logical addresses and physical addresses in the usual area and the secure area are managed as address information of the first memory.

7. The memory device according to claim 6, wherein the address information of the first memory includes boundary address information indicating the boundary between the authentication area and the non-authentication area and logical-physical address translation tables in the authentication area and the non-authentication area.

8. The memory device according to claim 6 or 7, wherein the boundary address information and the logical-physical address translation tables are recorded in an address information management area of the first memory.

9. The memory device according to claim 6, wherein the boundary between the usual area and the secure area represented by the boundary address information is changed according to a command of the electronic device authenticated by the secure control section.

10. The memory device according to claim 7, wherein the boundary between the authentication area and the non-authentication area represented by the boundary address information is changed according to a command of the electronic device authenticated by the general control section.

11. The memory device according to claim 10,

wherein the boundary address information of the boundary between the authentication area and the non-authentication area is made up of a real boundary address and an assumed boundary address set with the secure area excluded, and

wherein the real boundary address is changed based on the assumed boundary address specified by a command of the electronic device authenticated by the general control section.

12. An electronic device for accessing a memory device having a first area, a second area, and a third area as memory areas,

wherein upon reception of an access request to the memory device, the electronic device:

accesses the first area of a non-tamper-resistant memory area of the memory device through a general control section of the memory device for controlling access to the memory device;

after authenticated by the general control section and a secure control section of the memory device for controlling access to the second area and the third area, accesses the second area of a non-tamper-resistant memory area other than the first area through the secure control section; and

after authentication with the secure control section, accesses the third area of a tamper-resistant memory area of

the memory device through the general control section and the secure control section.

13. The electronic device according to claim 12, comprising:

first command generation means for generating a command for writing or reading data into or from the first area;

second command generation means for generating a command for requesting the secure control section to perform processing; and

first authentication processing means for acquiring an authentication key used for authentication with the secure control section and performing authentication processing with the secure control section.

14. The electronic device according to claim 12 or 13, wherein a non-authentication area of a partial area of the first area is accessed without authentication with the general control section and an authentication area of a part or all of the first area other than the non-authentication area is accessed after authentication with the general control section.

15. The electronic device according to claim 14, comprising:

third command generation means for generating a command for writing or reading data into or from the authentication

area; and

second authentication processing means for acquiring an authentication key used for authentication with the general control section and performing authentication processing with the general control section.